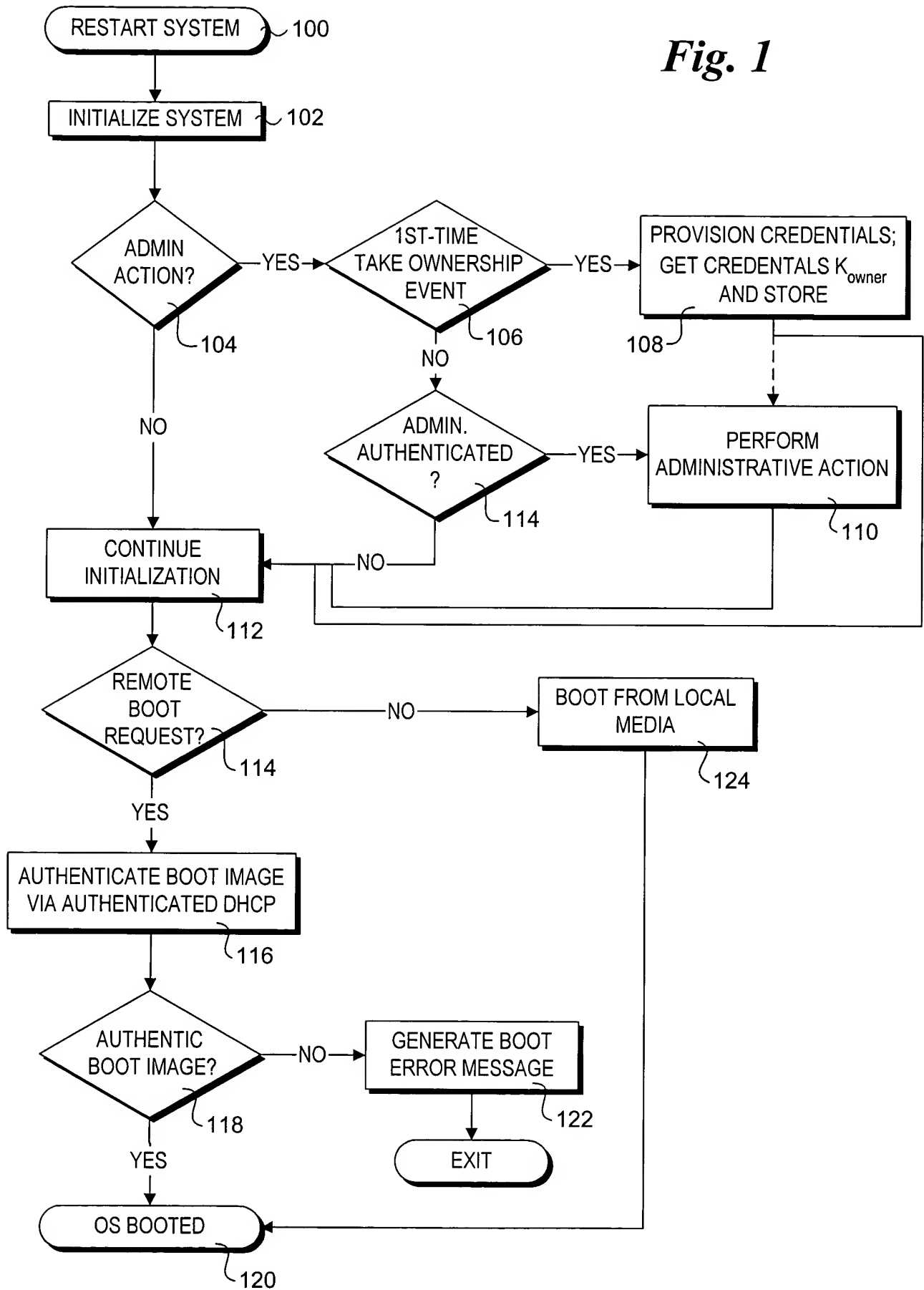
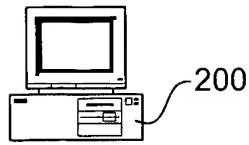
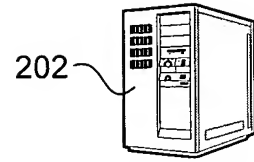


Fig. 1





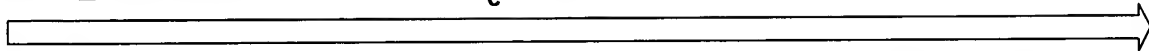
CLIENT



SERVER

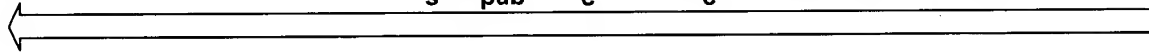
Nonce = N_c ,
 Password, Login
 $H_c = H(N_c + \text{password} + \text{Login})$

(DHCP_DISCOVER) N_c , Login



Nonce = N_s ,
 Password, Login, $K_{pub} = (n, e)$
 $H_s = H(N_s + \text{Password} + \text{Login})$

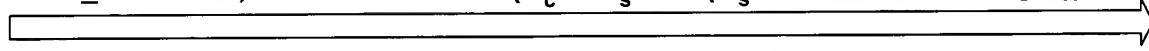
(DHCP_OFFER) N_s , K_{pub} , $H_c = H(N_c + \text{password} + \text{Login})$



if ($H_c \neq H_s$) (return "Authentication Error")

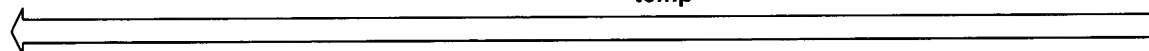
Nonce = N_c ,
 $K_{temp} = H(N_c + N_s + \text{Password} + \text{Login})$,

(DHCP_REQUEST) $T = Ek(N_c + H_s = H(N_s + \text{Password} + \text{Login}))$



N_c , H_s , after Public key Decryption
 if ($H_s \neq H_s$) (return "Authentication Error")
 Nonce = N_s ,
 $K_{temp} = \text{Hash}(N_c, N_s, \text{Password}, \text{Login})$
 $K_s = \text{Hash}(N_c, N_s, \text{password}, \text{Login})$

(DHCP_ACK) 3-DES (K_{temp}) (N_s')



$3\text{-DES}(K_{temp})(N_s') = N_s$,
 $K_s = \text{Hash}(N_c, N_s', \text{Password}, \text{Login}) = \text{Shared Secret Key}$

--- Loading the Bootp Image 3-DES (K_s) (TFTP Data)

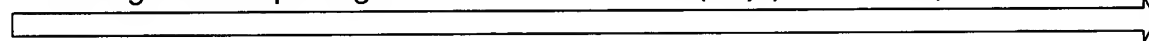


Fig. 2

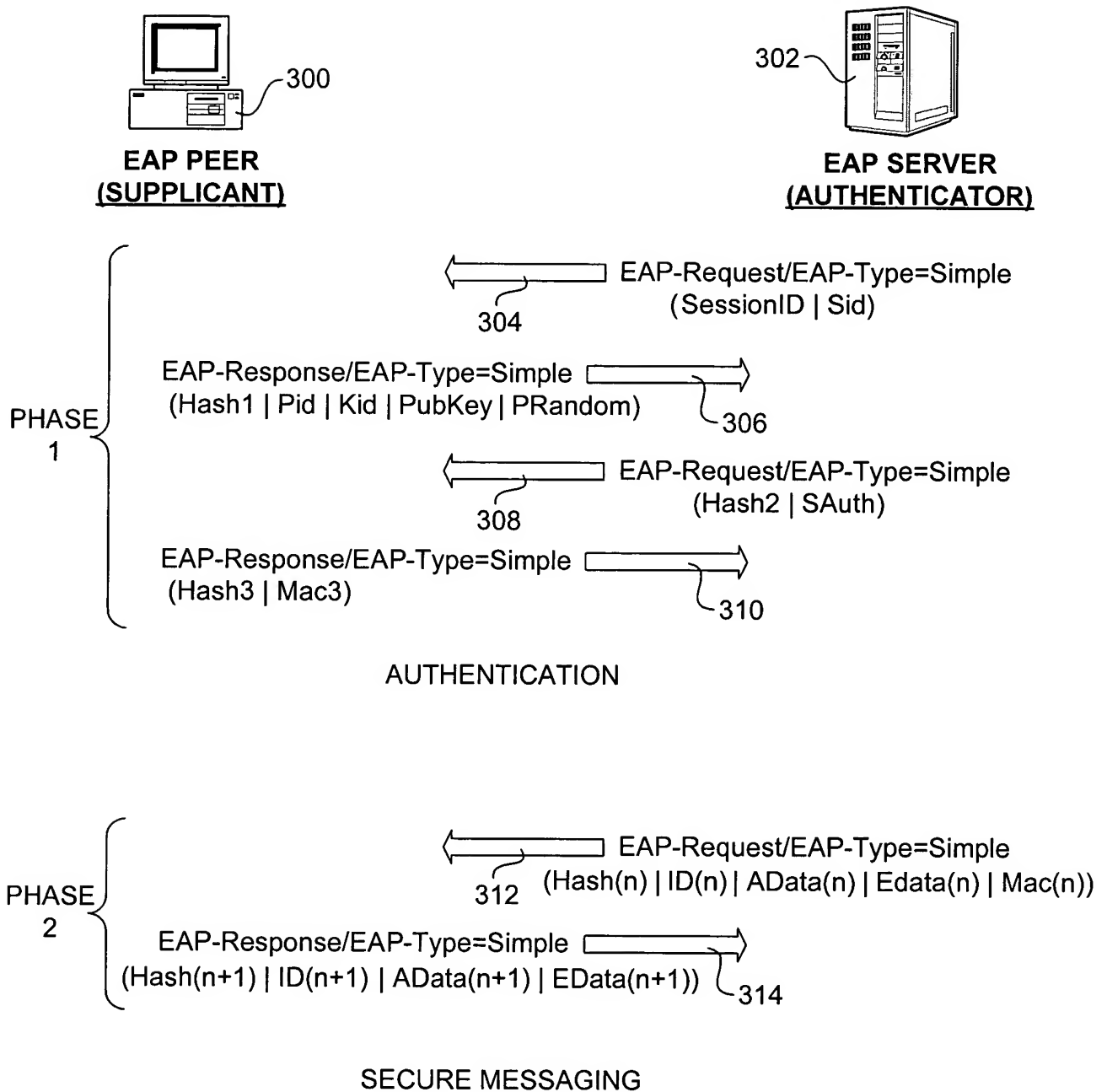


Fig. 3

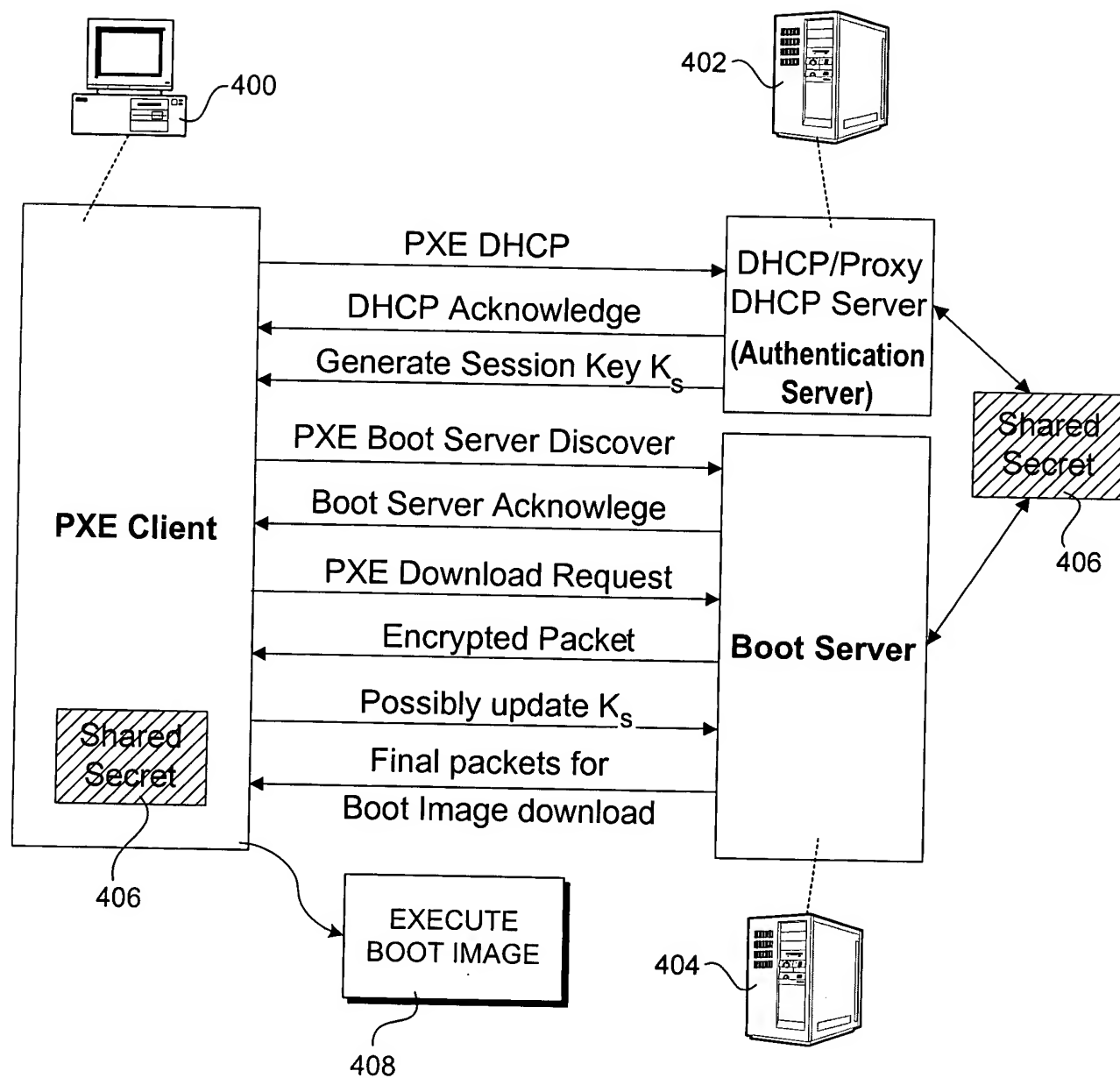


Fig. 4

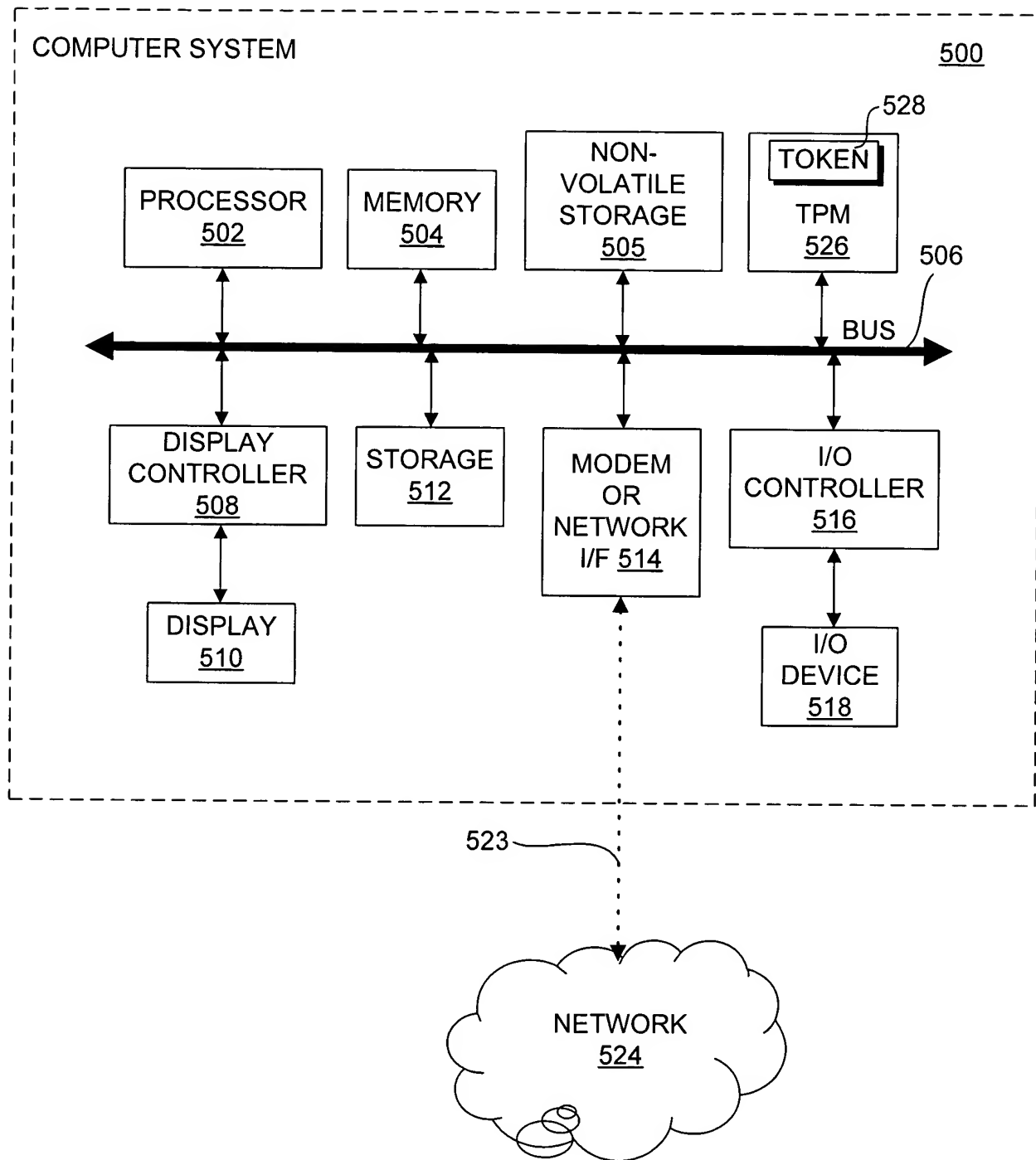


Fig. 5